

Державний вищий навчальний заклад
Донецький національний технічний університет
Кафедра прикладної математики та інформатики

«ЗАТВЕРДЖУЮ»

Перший проректор

_____ Леонід БАЧУРІН

«_____» _____ 2023 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ДВП 2.04 МЕТОДИ ТА ЗАСОБИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

(шифр і назва навчальної дисципліни)

Рівень освіти: перший (бакалаврський)

Спеціальність

121 Інженерія програмного забезпечення

(шифр і назва спеціальності (тей))

Освітня програма

Інженерія програмного забезпечення

(назва освітньої програми)

Мова навчання: українська

Робоча програма навчальної дисципліни «Методи та засоби технічного захисту інформації»
(повна назва дисципліни)
для здобувачів вищої освіти за спеціальністю 121 Інженерія програмного забезпечення
«24» 01 2024 року. – 9 с.

Розробник:
Ярослав ДОРОГИЙ, д.т.н., проф.,

Робоча програма затверджена на засіданні кафедри прикладної математики та інформатики
Протокол № 13 від “27” грудня 2023 р.

Завідувач кафедри прикладної математики та інформатики

_____ (Наталія МАСЛОВА)

“27” грудня 2023 р.

Схвалено науково-методичною комісією галузі знань 12 Інформаційні технології

Протокол № 1 від “15” 01 2024р.

Голова _____ (Євген БАШКОВ)

(підпис)

(прізвище та ініціали)

1. Загальна інформація

Форма навчання	Денна
Статус	Вибіркова
Обсяг в кредитах ЄКТС	5
Обсяг в годинах за навчальним планом, разом: в тому числі:	150
лекції:	48
практичні заняття:	32
самостійна робота:	70
Форма підсумкового контролю	Екзамен
Дисципліну викладають	Викладач проф. Дорогий Я.Ю., yaroslav.dorohyi@donntu.edu.ua ас. Нікітенко А.О. andrii.nikitenko@donntu.edu.ua

Передумови для вивчення дисципліни: успішному вивченню дисципліни «Методи та засоби технічного захисту інформації» сприяє попереднє опанування такими дисциплінами, як «Основи інформаційної безпеки», «Операційні системи».

2. Мета та предмет вивчення навчальної дисципліни «Методи та засоби технічного захисту інформації»

Навчальна дисципліна "Методи та засоби технічного захисту інформації" спрямована на формування у студентів необхідних знань і практичних навичок у галузі технічного захисту інформації в сучасних інформаційно-комунікаційних системах.

Мета цієї навчальної дисципліни полягає в тому, щоб забезпечити студентів технічними та методичними засобами для забезпечення безпеки обробки інформації в різних інформаційних системах. Основна увага приділяється вивченню технічних механізмів та інструментів захисту інформації, що входять до складу сучасних систем безпеки, удосконаленню професійної компетентності фахівців з технічного захисту інформації та забезпечення їхніх здатностей в контексті проведення обстеження об'єктів інформаційної діяльності, виявленні технічних каналів витоку інформації, розробці моделі загроз та технічного завдання щодо створення комплексних систем та комплексів технічного захисту інформації та передбачає оволодіння знаннями згідно з вимогами кваліфікаційного довідника професій працівників підрозділів технічного захисту інформації і забезпечує фахівцям теоретичні і практичні навички у справі організації технічного захисту інформації.

Завданням навчальних занять є ознайомлення студентів із сучасними методами технічного захисту інформації, вивчення їх принципів та застосування для практичного розв'язання завдань забезпечення безпеки інформації в різних контекстах. Це включає в себе аналіз технічних рішень для запобігання загрозам і виявлення вразливостей, а також розробку та впровадження заходів технічного захисту.

Компетентності:

ЗК01. Здатність до абстрактного мислення, аналізу та синтезу.

ЗК02. Здатність застосовувати знання у практичних ситуаціях.

ЗК06. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

ФК05. Здатність дотримуватися специфікацій, стандартів, правил і рекомендацій в професійній галузі при реалізації процесів життєвого циклу.

ФК06. Здатність аналізувати, вибирати і застосовувати методи і засоби для забезпечення інформаційної безпеки (в тому числі кібербезпеки).

ФК14. Здатність до алгоритмічного та логічного мислення.

Програмні результати навчання:

ПРН01. Аналізувати, цілеспрямовано шукати і вибирати необхідні для вирішення професійних завдань інформаційно-довідкові ресурси і знання з урахуванням сучасних досягнень науки і техніки.

ПРН10. Проводити передпроектне обстеження предметної області, системний аналіз об'єкта проектування.

ПРН11. Вибирати вихідні дані для проектування, керуючись формальними методами опису вимог та моделювання.

ПРН21. Знати, аналізувати, вибирати, кваліфіковано застосовувати засоби забезпечення інформаційної безпеки (в тому числі кібербезпеки) і цілісності даних відповідно до розв'язуваних прикладних завдань та створюваних програмних систем.

3. Очікувані результати навчання

Основними результатами опанування дисципліни «Методи та засоби технічного захисту інформації» є:

- здатність планувати й реалізувати відповідні заходи, щодо захисту інформації в інформаційних і комунікаційних системах;
- базові знання наукових понять, теорій і методів, необхідних для розуміння принципів роботи та функціонального призначення систем захисту інформації та безпеки інформаційно-комунікаційних систем;
- базові знання основних нормативно-правових актів та довідкових матеріалів, чинних стандартів і технічних умов, інструкцій та інших нормативно-розпорядчих документів з інформаційної безпеки;
- базові знання технічних характеристик, конструктивних особливостей, призначення і правил експлуатації систем технічного захисту інформації;
- здатність використовувати та впроваджувати нові технології, брати участь в модернізації та реконструкції обладнання, пристроїв, систем та комплексів, зокрема з метою удосконалення захищеності;
- здатність розуміти і враховувати соціальні, екологічні, етичні, економічні аспекти, що впливають на формування технічних рішень;
- здатність застосовувати професійно-профільовані знання й практичні навички для розв'язання типових задач спеціальності, а також експлуатації систем і засобів забезпечення захисту інформації з використанням необхідних видів, методів, засобів і технологій захисту;
- здатність використовувати уміння по виявленню й блокуванню каналів і методів несанкціонованого доступу до інформації, джерел і способів дестабілізуючого впливу на інформацію;
- здатність використовувати уміння по участі в підготовці технічної документації;
- уміння аргументувати вибір методів розв'язування спеціалізованих задач, критично оцінювати отримані результати та захищати прийняті рішення.

Внаслідок вивчення курсу студенти повинні:

знати:

- основні нормативно-правові акти, чинні стандарти та умови, інструкції з відповідної галузі;
- технічні характеристики, конструктивні особливості, призначення та правила експлуатації систем ТЗІ;
- основні підходи та методи по виявленню та блокуванню каналів і методів несанкціонованого доступу до інформації, джерел і способів дестабілізуючого впливу на інформацію;

вміти:

- розробляти та організовувати здійснення заходів для забезпечення захисту інформації з обмеженим доступом під час проведення всіх видів робіт усіма виконавцями підприємства, установи, організації;
- виконувати в установленому порядку роботи, пов'язані з технічним захистом інформації;
- аналізувати носії, склад і зміст інформації для визначення тієї її частини, котру потрібно захищати;
- розробляти та забезпечувати здійснення заходів для усунення причин і умов, які можуть створити умови для витоку інформації технічними каналами, та контролювати їх виконання;
- складати і оформляти офіційні документи, надавати кваліфіковані консультації.

4. Засоби діагностики результатів навчання

Засобами оцінювання та методами демонстрування результатів навчання при опануванні дисципліною «Методи та засоби технічного захисту інформації» передбачено:

- екзамен;
- індивідуальні завдання з практичних робіт.

5. Критерії оцінювання результатів навчання

Максимальний бал, визначений схемою оцінювання, наведеною нижче, можливо отримати за умови своєчасного та правильного виконання завдань. За наявності помилок або при несвоєчасному виконанні оцінка знижується до 60% від максимальної.

ПР 1	ПР 2	ПР 3	ПР 4	ПР 5	ПР 6	ПР 7	ПР 8	ПР 9	ПР 10	ПР 11	ПР 12	ПР 13	ПР 14	ПР 15	Поточний контроль	Іспит	Мах
2	3	2	3	2	3	2	3	2	3	2	3	2	5	3	40	60	100
1	2	1	2	1	2	1	2	1	2	1	2	1	3	2	24		

Примітки: 1) ПР1, ПР2 і т. д. лабораторні роботи;

2) У чисельнику максимальний бал – при своєчасному та правильному виконанні, у знаменнику – мінімальний (при правильному, але несвоєчасному виконанні)

Відповідність між шкалами встановлюється наступним чином:

Оцінка	
За 100-бальною шкалою	Для екзамену, курсового проекту (роботи), практики, диференційованого заліку, кваліфікаційного екзамену, випускної кваліфікаційної (дипломної) роботи (проекту)
90-100	відмінно

74-89	добре
60-73	задовільно
0-59	незадовільно

6. Програма навчальної дисципліни

6.1. Основні теми дисципліни

Змістовний модуль 1. Нормативно-правові основи технічного захисту інформації.

Тема 1. Вступ до дисципліни. Нормативно-правові основи технічного захисту інформації.

Тема 2. Побудова комплексу технічного захисту інформації.

Тема 3. Технічні засоби захисту інформації.

Змістовний модуль 2. Технічні канали витоки інформації

Тема 4. Технічні канали витоку інформації.

Тема 5. Розвідка та добування інформації.

Тема 6. Закладні пристрої.

Тема 7. Засоби виявлення каналів витоку інформації.

Змістовний модуль 3. Захист та протидія витоку інформації

Тема 8. Пристрої захисту та протидії витоку.

Тема 9. Методи захисту інформації оброблюваної ТЗПІ від витоку технічними каналами.

Змістовний модуль 4. Технічний захист інформації в комп'ютерних системах і мережах.

Тема 10. Захист інформації в комп'ютерних системах і мережах.

Змістовний модуль 5. Технічний захисту інформації в комунікаційних мережах і системах зв'язку.

Тема 11. Захист інформації в комунікаційних мережах.

Тема 12. Захист інформації в мережах зв'язку.

6.2. Теми лабораторних занять

Лабораторні роботи не передбачено планом.

6.3. Теми практичних занять

№ п/п	Тема і зміст практичних занять	Обсяг практичних занять (ак. год.) для денної форми навчання
1	Нормативно-правова база технічного захисту інформації (Тема 1)	2
2	Підсистема фізичного захисту джерел інформації (Тема 2)	2
3	Класифікація методів технічного захисту інформації (Тема 3)	2
4	Проектування комплексу ТЗІ (Тема 2,3)	4
5	Паразитні зв'язки та наведення (Тема 4,5)	2

6	Низькочастотні та високочастотні випромінювання технічних засобів (Тема 4,7)	2
7	Засоби телевізійного спостереження (Тема 5)	2
8	Диктофони. Закладні (заставні) пристрої. Лазерні засоби підслуховування. Засоби високочастотного нав'язування (Тема 5)	2
9	Характеристики радіоприймачів. Технічні засоби аналізу сигналів. Засоби визначення координат джерел радіосигналів. Засоби перехоплення оптичних та електричних сигналів (Тема 5,7)	2
10	Демаскуючі ознаки сигналів. Демаскуючі ознаки речовин (Тема 7)	2
11	Засоби контролю приміщень на відсутність закладних пристроїв (Тема 6-9)	2
12	Джерела загроз випадкових впливів. Чинники забезпечення захисту від загроз впливу. Чинники забезпечення захисту інформації від загроз витоку (Тема 9)	2
13	Засоби контролю телефонних ліній та ланцюгів електроживлення (Тема 8,9, 12)	2
14	Запобігання витоку інформації з ланцюгів електроживлення та заземлення (Тема 8-12)	2
15	Оцінка загроз радіоелектронних та речових каналів витоку інформації (Тема 10)	2
	Всього практичних занять	32

6.4. Самостійна робота

№ з/п	Назва теми	Кількість годин для денної форми навчання
1	Тема 1. Вступ до дисципліни. Нормативно-правові основи технічного захисту інформації.	2
2	Тема 2. Побудова комплексу технічного захисту інформації.	10
3	Тема 3. Технічні засоби захисту інформації.	10
4	Тема 4. Технічні канали витоку інформації.	10
5	Тема 5. Розвідка та добування інформації.	6
6	Тема 6. Закладні пристрої.	6
7	Тема 7. Засоби виявлення каналів витоку інформації.	6
8	Тема 8. Пристрої захисту та протидії витоку.	6
9	Тема 9. Методи захисту інформації оброблюваної ТЗПІ від витоку технічними каналами.	6
10	Тема 10. Захист інформації в комп'ютерних системах і мережах.	8
11	Тема 11. Захист інформації в комунікаційних мережах.	8
12	Тема 12. Захист інформації в мережах зв'язку.	8
	Разом	86

6.5. Індивідуальне завдання

Не передбачено навчальним планом

7. Література

7.1. Основна

1. М. В. Грайворонський, О. М. Новіков. Безпека інформаційно-комунікаційних систем. – К.: Видавнича група ВНУ, 2009. – 608 с.
2. Методи та засоби технічного захисту інформації: Опорний конспект лекцій [Електронний ресурс] : навч. посіб. для студ. спец. 125 «Кібербезпека» / КПІ ім. Ігоря Сікорського ; уклад.: В.М. Луценко, Д.О. Прогонов. – Електронні текстові дані (1 файл: 1,80 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2021. – 289 с.

7.2. Додаткова

1. ДСТУ 3396.0-96.
2. ДСТУ 3396.1-96.
3. ДСТУ 3396.2-97.
4. НД ТЗІ 3.7-003-2005 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.
5. НД ТЗІ 1.1-005-07 «Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення»
6. НД ТЗІ 3.1-001-07 «Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Передпроектні роботи»
7. НД ТЗІ 3.3-001-07 «Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Порядок розроблення та впровадження заходів із захисту інформації».
8. НД ТЗІ 2.1-002-07 «Захист інформації на об'єктах інформаційної діяльності. Випробування комплексу технічного захисту інформації. Основні положення».
9. ТПКО-95 Тимчасове положення з категоріювання ОІД.
10. ДБН А.2.2-2-96 ДЕРЖАВНІ БУДІВЕЛЬНІ НОРМИ УКРАЇНИ. Проектування. Технічний захист інформації. Загальні вимоги до організації проектування і проектної документації для будівництва.
11. Положення про державний контроль за станом технічного захисту інформації від 16.05.2007 №87.

7.3. Методична

1. Методи та засоби технічного захисту інформації. Конспект лекцій. [Електронне видання] / Уклад.: Я.Ю. Дорогий. – Л.: ДВНЗ «ДонНТУ», 2024.
2. Методи та засоби технічного захисту інформації. Методичні вказівки до виконання практичних занять. [Електронне видання] / Уклад.: А.О. Нікітенко, Я.Ю. Дорогий. – Л.: ДВНЗ «ДонНТУ», 2024.

8. Інформаційні ресурси

1. Operating System Fundamentals. – [Електронний ресурс] – Режим доступу: <https://www.coursera.org/programs/program-natsional-nii-tiekhnichnii-univiersitiet-ukrayini-kiyivs-kii/learn/akamai-operating-systems>.
2. Linux Server Management and Security. - [Електронний ресурс] – Режим доступу: <https://www.coursera.org/programs/program-natsional-nii-tiekhnichnii-univiersitiet-ukrayini-kiyivs-kii/learn/linux-server-management-security>.
3. Windows Server Management and Security. - [Електронний ресурс] – Режим доступу: <https://www.coursera.org/programs/program-natsional-nii-tiekhnichnii-univiersitiet-ukrayini-kiyivs-kii/learn/windows-server-management-security>.